UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,684	01/04/2007	Yuichi Futa	2006_0401A	3546

52349 7590 10/09/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/573,684	FUTA ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5,10-12 and 14-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 5, 10-12, and 14-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/573684 is presented for examination by the examiner. Claim 4 has been canceled. Claims 14-17 have been added. Claims 1, 2, 5, 10-12, and 14-17 are pending.

Response to Amendment

Claims have been amended to overcome the previous 112 rejections.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Now that canceled claim 4's limitations have been incorporated into claim 2, claim 5 is indefinite. Claim 5 contradicts the limitation in claim 2 wherein the communication device concatenates the first and second keys to generate concatenated data and calculates a hash value for the concatenated data and generates the encryption and hash key from this hash value. Claim 5 says the first and second key are XOR'd together to generate the encryption and hash keys. Its unclear how this could occur since the first and second key are already concatenated together to produce the encryption and hash key.

Response to Arguments

Claim Objections

Previous claim objections have been withdrawn due to persuasive arguments.

Claim Rejections

Applicant's arguments filed 6/29/09 have been fully considered but they are not persuasive. Applicant has essentially argued that the combination of Diffie, Bellare, and Morais fail to teach the newly amended independent claims. Examiner respectfully disagrees.

First, the independent claims are interpreted by the following summary. The process starts by doing a key exchange where the first device sends its key part under the protection of the second device's public key to the second device. The first device receives the second device's key part encrypted with the first device's public key. Now the first device has both key parts. The same process is carried out for the second device so it possesses the same two key parts. Diffie teaches this process as highlighted in the 103 rejection below.

The claim then describes how the two key parts are manipulated to create an encryption key and a hash key. Diffie teaches generating an encryption key from the two parts (col. 2, line 10). However, Morais teaches that two independent key parts can be concatenated together and then hashed to form other keys and hashing algorithms (0045-0046). This reads on the claims' concatenation and hashing of the first and

second keys to generate a hash value. Per the claims, the encryption and hash key are derived from this hash value. Morais specifically teaches generating an encryption key from the hash of the two key concatenation (0045; LAN key). This LAN key is the output of the two key concatentation hash function. Morais teaches the LAN key is then used to create shared secret keys and keys for hashing algorithms (0046). The only process still missing from the claims is the creation/use of a hash key. Diffie teaches it is important to check the integrity and privacy of packets transmitted via a checksum. MACs are well known and are more secure substitutes for checksums. MACs inherently require a hash key. Bellare teaches about using keying hashing functions for message authentication. Diffie teaches the need to protect the integrity of a packet, Morais teaches two keys can be concatenated together and hashed to generate hashing algorithms, and Bellare pulls it all together by teaching MACs are known to protect the integrity of packets with a hash key. Given these three teachings, it would have obvious to generate and use the hash key in the way described by the claims. It is also inherent that if you are going to create a MAC from the data, you send its value so the receiver can check the validity and authenticity of the data.

In view of this, Examiner maintains that the combination of Diffie, Morais, and Bellare render the claims obvious. Given the key exchange of Diffie, it would have been obvious to combine the key parts as taught by Morais, and implement a MAC as taught by Bellare.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 10-12, and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 5,371,794 to Diffie et al., hereinafter Diffie in view of USP Application Publication 2003/0093669 to Morais et al., hereinafter Morais and in view of "Keying Hash Functions for Message Authentication", 1996 publication by Bellare et al., hereinafter Bellare.

As per claims 1, 2, 11, and 12, Diffie teaches a communication system, device, and method between a first device and a second device, wherein the first device [base] (i) encrypts a 1st key [RN1] using a public key of the second device [mobile] to generate 1st encrypted data, and transmits the 1st encrypted data to the second device (col. 7, lines 50-65)),

(ii) receives 2nd encrypted data from the second device, and decrypts the 2nd encrypted data using a secret key of the first device to obtain a 2nd key [RN2], and (col. 8, lines col. 49-53))

(iii) generates, based on the 1st and 2nd keys, a 1st encryption key [session key] for use in communication with the second device, the second device (col. 8, lines 65-67)

(i) encrypts a 3rd key [RN2] using a public key of the first device to generate the 2nd encrypted data, and transmits the 2nd encrypted data to the first device (col. 8, lines 49-57)),

(ii) receives the 1st encrypted data from the first device, and decrypts the 1st encrypted data using a secret key of the second device to obtain a 4th key [RN1] (Fig. 5a and col. 8, lines 44-45), and

(iii) generates, based on the 3rd and 4th keys, a 2nd encryption key [session key] for use in communication with the first device (col. 8, line 47-49), and the first and second devices perform encrypted communication using the 1st and 2nd encryption keys (col. 8, lines 47-49),

wherein the first device generates the first encryption key based on the first and second keys (col. 8, lines 65-67).

Diffie teaches the first device encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the encrypted first transmission data to the second device (col. 9, lines 15; session key is obtained, inherently used to encrypt data). Diffie teaches the second device generates the second encryption key based on the third and fourth keys (col. 8 ,lines 47-49), receives from the communication device the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key (col. 9, lines 15; session key is obtained, inherently used to decrypt data). Again Diffie's invention is directed to two parties obtaining a session key whereby data may be encrypted and decrypted.

Diffie teaches the first and second keys RN1 and RN2 are known to each side of the communication. In fact they jointly arrive at these keys. While the claims label the second device's keys as the third and fourth keys, they are in fact the same as the first and second keys. Diffie does not explicitly teach the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value.

Morais teaches the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key [LAN key or other secret keys] and the hash key [for hashing algorithms] based on the hash value [LAN key is the generated hash value; 0045-46]. Diffie teaches using XOR to combine the key parts. Concatenation as taught by Morais of key parts is yet another way to logically combine keys to arrive at another key. This is just a simple substitution of a known function and as such it would have been obvious to one of ordinary skill in the art at the time of the invention to substitute another known logical way of combining keys.

Diffie teaches the use of a encrypted check sum field but is silent in teaching creating a first/second hash key (same key) and using the hash key to hash the data to create a hash value, sending this hash value to the second device so that it may verify that the data has not been tampered with.

The use of MACs and their corresponding keys is well known in the art. In order for MAC to work both sides need to know the key being used. Bellare teaches the MAC

algorithm in section 1.4 starting on page 4. This MAC algorithm uses a secret key in the generation of the MAC. MACs again are known in the art to provide tampering evidence. It is within the capabilities of one of ordinary skills in the art to substitute known methods for known purposes which result in predictable results. The claims are obvious because one of ordinary skill in the art could have substituted the MAC algorithm for the check sum to increase the security of the system. The use of a MAC is more secure than simple check sums. The combining rationale of Diffie and Bellare is to use a MAC for message authentication because it is more secure than a checksum. The hash key as generated by the combination of Diffie and Morais would then be used to generate hash values (MAC). Morais generates the MAC key in a particular way which combines well with Diffie because of the two key parts. Ultimately though, the hash key is just a hash key and is used in the traditional way described by Bellare. The second device would then receive the resulting hash value [first hash value] and compare that value to its own hash value [second hash value] which is calculated by hashing the received data with its copy of the hash key. Substituting this teaching into the combination of Diffie and Morais would render the claims obvious. Furthermore the session key of Diffie [first/second encryption key] is distinct from the hash key.

As per claim 5, the combined system of Diffie, Morais, and Bellare teaches the key generation unit performs an exclusive OR operation using the 1st and 2nd keys (Diffie, col. 8, lines 47), and generates the encryption key and the hash key based on a result of the operation. Diffie XOR's the key parts to create the session key. Examiner

relies on the rationale to combine Diffie and Bellare as disclosed above for using a hash key.

As per claim 10, Diffie teaches the data generation [packet] unit encrypts the 1st key [RN1] based on a key encapsulation mechanism to generate the 1st encrypted key data, and the decryption unit decrypts the 2nd encrypted key data based on a key decryption mechanism to obtain the 2nd key [RN2] (col. 9, lines 57-63).

As per claims 14-17, Diffie is silent in disclosing the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys. Morais teaches the first encryption key and the first hash key are included in a hash calculation result that is generated by performing a hash calculation using the concatenated data generated by concatenating the first and second keys (0045-46). The LAN key, which is the hash value of the two key concatenation-hash, is used to generate session keys and hashing algorithms. Examiner supplies the same rationale to combine Morais with Diffie as recited in the rejection of claim 1.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431